Red Hat Directory Server 8.2 Release Notes

Updated for Errata RHBA-2012:0064
Edition 8.2.8

Landmann

Red Hat Directory Server 8.2 Release Notes

Updated for Errata RHBA-2012:0064
Edition 8.2.8

Landmann
rlandmann@redhat.com

Abstract

Release notes for Directory Server 8.2.

Table of Contents

These release notes contain important information available at the release of Red Hat Directory Server version 8.2. New features, system requirements, installation notes, known problems, resources, and other current issues are addressed here. Read this document before beginning to use Directory Server 8.2.

1. New Features in Red Hat Directory Server 8.2

Directory Server 8.2 has introduced many features to make managing the directory service and its data easier.

1.1. Setting Limits for Anonymous Users

Previously, it was impossible to set resource limits on anonymous users. Resource limits could only be set on users who existed in the directory. Since anonymous binds didn't correspond to a user entry, only general Directory Server settings could be applied to anonymous operations. A new attribute, ***nsslapd-anonlimitsdn***, references a template entry that can be used to define resource limits. All anonymous binds are treated as that template entry.

For additional security, the new ***nsslapd-allow-anonymous-access*** attribute can be set to **off** to disable anonymous binds entirely.

1.2. Requiring Secure Connections for Simple Bind

A simple bind is a bind attempt which uses a username-password combination to authenticate to the server. The vulnerability in simple binds is that the password is transmitted in plaintext. The new ***nsslapd-require-secure-binds*** attribute requires that simple binds occur only over a secure connection (TLS, SASL, or Start TLS).

1.3. Mixing SASL and TLS Connections

In other versions of Directory Server, the server could not be configured to connect over both SASL and TLS simultaneously. In Red Hat Directory Server 8.2, the server can now have both SASL and TLS configured and the desired protocol can be used for different server connections.

1.4. Requiring a Minimum Security Strength Factor for Server Connections

The security of the connection is determined by its *security strength factor*. New configuration and ACI parameters allow administrators to set the minimum key strength required to process operations.

In Red Hat Directory Server 8.2, it is possible to require operations to occur over a connection with a certain level of security. The ***nsslapd-minssf*** attribute sets the required security factor. The new **ssf** keyword for ACIs allows access control rules to be set that require certain operations or users to meet security strength factors.

1.5. Adding Entry Update Sequence Numbers (USN) for Write Operations

The Entry USN Plug-in provides a way for LDAP clients to know that something in the database has changed. This plug-in generates a global update sequence number (USN) for an entry whenever a write operation occurs.

A new operational attribute, ***entryusn***, stores the latest USN for an entry. This value is calculated globally, much like change sequence numbers for replication. So, if entry A is updated and has an ***entryusn*** of 1, and then entry B is updated, entry B has an***entryusn*** value of 2. Another attribute, ***lastusn***, is kept on the root DSE which shows the most recent USN number assigned to any entry in

the directory, and thus the most recent change number.

1.6. Generating Links Between Entry Attributes

Linking attributes allows Directory Server to express and maintain relationships between entries dynamically. The Linked Attribute Plug-in uses the DN value of an attribute to trace its way to the related entry, and then it adds a reciprocal value on that entry. This is similar to the way that classes of service dynamically generate values from a template entry, only no template is necessary.

For example, a manager and his direct report have a relationship. Whenever the Directory Manager adds a ***manager*** attribute to a user entry, the Linked Attributes Plug-in follows that DN to the relate entry, and then adds a ***directReport*** attribute to the manager's user entry.

1.7. Validating Attribute Syntax

Syntax validation verifies that the value given for an attribute matches the required syntax for that attribute. If the value is of the wrong syntax, then the modify operation fails.

New scripts have been added to validate the syntax of existing attributes.

1.8. Added Support for Dereferencing Searches

A dereferencing search is a quick way to track back over cross-references in an entry and return information about the referenced entry. Dereferencing simplifies many client operations. Some operations may require getting a list of cross-links from one entry and then performing a second series of searches to get information from the entries referenced in the list. Dereferencing allows those sequences of searches to be consolidated into a single search.

Directory Server 8.2 now supports the dereferencing control for search operations. When the dereferencing control and search information is passed with a search, Directory Server can perform the series of searches required.

IMPORTANT

The dereferencing searches are not done using MozLDAP command-line tools. The server supports dereferencing search operations; however, the client tools with Red Hat Directory Server do not. Therefore, dereferencing operations must be done using OpenLDAP command-line tools version 2.4.18 or later or other clients which support dereferencing searches.

1.9. Added Support for Bitwise Filters

Directory Server 8.2 introduces support for searching for attributes with bit field values, both for bitwise AND and bitwise OR searches.

Bit field values are common in Windows attributes. Search support for bitwise attribute values helps integration between Red Hat Directory Server, Red Hat Enterprise Linux, and Windows-related applications, such as Samba file servers.

1.10. Enhanced Searches for Simple Paged Results

Simple paged results is a control that breaks search results into pages of a certain length. In Directory Server 8.2, this is implemented as a ***supportedControl***. Much like virtual list views, simple paged results parcel very large search results into manageable sizes. Simple paged results can be scrolled through; the full behavior of the control is described in RFC 2696.

IMPORTANT

The simple paged results are not done using MozLDAP command-line tools. The server supports simple paged search operations; however, the client tools with Red Hat Directory Server do not. Therefore, simple paged operations must be done using OpenLDAP command-line tools version 2.4.18 or later or other clients which support simple paged results.

1.11. Configuring the Execution Order for Plug-ins

Generally, plug-ins are not called in a specific order. As in, it is not possible to define that Preoperation Plug-in A is always called before Preoperation Plug-in B. It can be convenient, however, to set one preoperation or postoperation plug-in to complete its job before the next plug-in is executed. This can allow more complex interactions between plug-ins and more specific functionality for plug-ins.

A new plug-in configuration attribute, ***nsslapd-pluginPrecedence*** has been added which sets the load order preference for the plug-in, anywhere from 1 to 99. The smaller the number, the higher the precedence.

IMPORTANT

Changing the execution order of the default plug-ins in Red Hat Directory Server is *not* supported and is strongly discouraged. Core functionality should not be altered.
This new feature is intended to set the execution order of custom plug-ins to add more flexibility to deploying custom functionality.

1.12. Using a Named Pipe in Place of Server Logs

Many administrators want to do some special configuration or operation with logging data, like configuring an access log to record only certain events. This is not possible using the standard Directory Server log file configuration attributes, but it is possible by sending the log data to a named pipe, and then using another script or plug-in to process the data. Using a named pipe for the log simplifies these special tasks, like:

- Logging certain events, like failed bind attempts or connections from specific users or IP addresses
- Logging entries which match a specific regular expression pattern
- Keeping the log to a certain length (logging only the last number of lines)
- Sending a notification, such as an email, when an event occurs

A new script, **`ds-logpipe.py`**, has been added to the Directory Server command-line tools to enable logs to be replaced by a named pipe.

1.13. Adding Support for Using PAM for Pass-THrough Authentication

A new plug-in allows administrators to use the pluggable authentication module (PAM) configuration within existing infrastructure for pass-through authentication for Directory Server users.

1.14. Upgrading DN Syntax to Comply with RFC 4514

In Red Hat Directory Server 8.0 and 8.1, DN syntax was defined by standards like RFC 2253. In Red Hat Directory Server 8.2, DNs are validated against the more strict syntax in RFC 4514. This means that

entries, possibly even entire directory trees, that were valid in Directory Server 8.0 or 8.1 are invalid and rejected in Red Hat Directory Server 8.2.

As part of the upgrade process (**`setup-ds-admin.pl -u`**), Directory Server runs a script to normalize and update the DNs in existing directories so that they conform with RFC 4514. Probably the most common change is escaping characters like quotation marks and commas in ***cn*** and ***ou*** elements in DNs, as well as some international characters. For example, replication agreement entries and other mapping tree entries have suffixes in the DN as one of the ***cn*** elements.

In 8.1, a replication entry DN would have the suffix name contained in quotes:

```
dn: cn=ExampleAgreement,cn=replica,cn="dc=example,dc=com",cn=mapping
tree,cn=config
```

If that same entry were created in Directory Server 8.2, there are no quotation marks are removed and the commas are escaped:

```
dn: cn=ExampleAgreement,cn=replica,cn=dc=example\,dc=com,cn=mapping
tree,cn=config
```

To preserve backward compatibility, migrated entries are stored with special characters encoded in the DN and ***entrydn*** attributes but otherwise preserved. For example, for a DN which was previously **`cn="a=abc,x=xyz"`**:

```
/usr/lib64/mozldap/ldapsearch -b "dc=example,dc=com" '(cn=\"*\")' entrydn
dn: cn=a\3Dabc\2Cx\3Dxyz,dc=example,dc=com
entrydn: cn=a\3dabc\2cx\3dxyz,dc=example,dc=com
cn: "a=abc,x=xyz"
```

The DN has the encoded value, but the CN preserves the special characters.

New entries in Directory Server 8.2 use the new DN format.

1.15. Expanded Support for Matching Rules and Attribute Syntaxes

Directory Server 8.2 introduces support for several new matching rules, so that Red Hat Directory Server now supports almost all of the matching rules listed in RFC 4517, with the exception of the FirstComponent matching rules.

Support was added for eleven new attribute syntaxes as well:

- Numeric String
- Bit String
- Delivery Method
- Enhanced Guide
- Facsimile Telephone Number
- Fax
- Guide
- Name and Optional UID
- Printable String
- Teletex Terminal Identifier
- Telex Number

1.16. Enhanced Start Scripts for the Directory Server, Admin Server, and SNMP Service

New start scripts have been added for the Directory Server, Admin Server, and SNMP services. Additionally, a new configuration file template has been added for the SNMP service.

1.17. Support for Salted MD5 Password Hash

Passwords can now be stored with the salted MD5 password hash. This provides more compatibility with users that are migrated from other directory services.

1.18. Expanded Documentation

Several enhancements have been made to the Red Hat Directory Server manuals:

- The documentation set has been expanded to include a new *Performance Tuning Guide*. This guide builds on the performance tuning chapter in the *Administrator's Guide*.
- A new chapter has been added to the *Administrator's Guide* to cover disaster recovery procedures.
- A new section describing how to use PAM pass-through authentication has been added to the *Administrator's Guide*.

2. Structural Changes in Red Hat Directory Server 8.2

There have been some changes in Red Hat Directory Server 8.2 in how the server handles DN formats.

2.1. Enforced DN Compliance with RFC 4514

Previous versions of Directory Server used older RFCs for DN formats and compliance. Red Hat Directory Server 8.2 enforces the stricter RFC 4514 for DN formats. As part of the upgrade script, existing DNs are reformatted to be properly encoded in line with RFC 4514.

For example, quotation marks in DNs must be properly escaped. For a DN which was previously **cn="a=abc,x=xyz"**, the updated format escapes the quotation marks as follows:

```
cn=a\3Dabc\2Cx\3Dxyz,dc=example,dc=com
```

2.2. No Longer Allowing Duplicate DNs

Directory Server 8.1 allowed entries with identical DNs, but slightly different DN formats, to be added to the directory. For example:

```
dn: cn="uid=jsmith,ou=Dev0,o=Engineering0",ou=People,dc=example,dc=com
uid: jsmith
givenName: test
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetorgperson
sn: smith
cn: uid=jsmith,ou=Dev0,o=Engineering0
userPassword: secret

dn: cn=uid\=jsmith\,ou\=Dev0\,o\=Engineering0,ou=People,dc=example,dc=com
uid: jsmith
givenName: test
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetorgperson
sn: smith
cn: uid=jsmith,ou=Dev0,o=Engineering0
userPassword: secret
```

When these duplicate entries are migrated and their DNs are upgraded to the new, stricter DN format after running **setup-ds-admin.pl -u**, the duplicate entry is given a slightly differnet DN that incorporates its unique ID. After the server upgrade, these duplicate entires can be preserved (which takes up additional space) or they can be purged.

1. Open the error log for the instance.

   ```
   vim /var/log/dirsrv/slapd-instance_name/error
   ```

2. Look for error messages related to duplicate entries. These messages will have the term *Duplicated entrydn* or *Duplicated entry* in them. For example:

   ```
   [..] - upgradedn userRoot: Duplicated entrydn detected:
   "cn=uid\3djsmith1\2cou\3ddev0\2co\3dengineering0,ou=people,dc=example,dc=com
   ": Entry ID: (10, 11)
   [..] - upgradedn userRoot: WARNING: Duplicated entry
   cn=uid\=jsmith1\,ou\=Dev0\,o\=Engineering0,ou=People,dc=example,dc=com is
   renamed to
   cn=uid\3Djsmith1\2Cou\3DDev0\2Co\3DEngineering0+nsuniqueid=ae8c95af-8fac11df-
   80000000-00000000,ou=People,dc=example,dc=com; Entry ID: 11
   ```

3. Decide which duplicated entry to keep. One entry will have the standard DN. The other has an RDN in the format **cn=***cn+nsuniqueid*.
4. Delete the duplicate entries. Each specific duplicate entry must be deleted manually. For example:

   ```
   /usr/lib64/mozldap/ldapdelete -D 'cn=directory manager' -w secret

   dn:
   cn=uid\3djsmith1\2cou\3ddev0\2co\3dengineering0,ou=people,dc=example,dc=com
   ```

5. If the entry which was kept has the renamed RDN format (**cn=***cn+nsuniqueid*), then rename the entry to the original DN. For example:

```
/usr/lib64/mozldap/ldapmodify -D "cn=directory manager" -w secret -p 389

dn: cn=uid\3Djsmith1\2Cou\3DDev0\2Co\3DEngineering0+nsuniqueid=ae8c95af-
8fac11df-80000000-00000000,ou=People,dc=example,dc=com
changetype: modrdn
newrdn: cn=uid\3djsmith1\2cou\3ddev0\2co\3dengineering0
deleteoldrdn: 0
```

NOTE

The ***deleteoldrdn*** value must be 0 since the nsuniqueid operational attribute cannot be deleted.

3. System Requirements

This section contains information related to installing and upgrading Red Hat Directory Server 8.2, including prerequisites and hardware or platform requirements.

3.1. Required JDK

Red Hat Directory Server 8.2 requires Sun JRE 1.6.0 or OpenJDK 1.6.0 for Red Hat Enterprise Linux 4 and 5.

IMPORTANT

It is not possible to manage instances of Directory Server older than 8.1 (which used JDK 1.5) with the 8.2 Directory Server Console because they are using different JDK versions.

3.2. Directory Server Supported Platforms

Directory Server 8.2 is supported on the following platforms:

- Red Hat Enterprise Linux 4 x86 (32-bit)
- Red Hat Enterprise Linux 4 x86_64 (64-bit)
- Red Hat Enterprise Linux 5 x86 (32-bit)
- Red Hat Enterprise Linux 5 x86_64 (64-bit)
- Solaris 9 SPARC (64-bit)

NOTE

Red Hat Directory Server 8.2 is supported running on a virtual guest on a Red Hat Enterprise Linux virtual server.

3.3. Directory Server Console Supported Platforms

The Directory Server Console is supported on the following platforms:

- Red Hat Enterprise Linux 4 i386 (32-bit)

- Red Hat Enterprise Linux 4 x86_64 (64-bit)
- Red Hat Enterprise Linux 5 i386 (32-bit)
- Red Hat Enterprise Linux 5 x86_64 (64-bit)
- Solaris 9 SPARC (64-bit)
- Windows XP Professional
- Windows Server 2003
- Windows Server 2008 (32-bit)
- Windows Server 2008 (64-bit)

3.4. Password Sync Service Platforms

The Password Sync Service runs on these Windows platforms:

- Windows Server 2003
- Windows Server 2008 (32-bit)
- Windows Server 2008 (64-bit)

3.5. Web Application Browser Support

Directory Server 8.2 supports the following browsers to access web-based interfaces, such as **Admin Express** and online help tools:

- Firefox 3.x
- Microsoft Internet Explorer 6.0 and higher

4. Installing Directory Server 8.2

For more detailed instructions on installing Directory Server 8.2, see the *Directory Server Installation Guide*.

4.1. Installing the JDK

Directory Server 8.2 requires either Sun JRE 1.6.0 or OpenJDK 1.6.0.

For example, to install OpenJDK on Red Hat Enterprise Linux 5:

```
yum install java-1.6.0-openjdk
```

OpenJDK is also available for download from http://openjdk.java.net/install/.

IMPORTANT

It is not possible to manage instances of Directory Server older than 8.1 (which used JDK 1.5) with the 8.2 Directory Server Console because they are using different JDK versions.

4.2. Installing Packages

There are two ways to install Red Hat Directory Server packages:

- Downloading RPMs or ISOs from Red Hat Network

- Using **up2date** or **yum** to pull the packages from the Red Hat Network repository

Downloading Packages from Red Hat Network

Red Hat Directory Server 8.2 packages are available for download from Red Hat Network (http://rhn.redhat.com). Downloading packages from Red Hat Network requires specific entitlements for the account for the 8.2 release.

1. Log into Red Hat Network.
2. Open the Red Hat Directory Server 8.2 channel in **Channels**, and go to the **Downloads** tab.
3. Download the packages.

   Both RPMs and ISO images are available for download through Red Hat Network, along with tarball packages (**.tar.gz**) of the source code.

   The ISO images for Red Hat Enterprise Linux can be downloaded and burned on to a CD-recordable media using the appropriate software.

   

   NOTE

   There are two PassSync packages available, one for 32-bit Windows servers and one for 64-bit. Make sure to select the appropriate packages for your Windows platform.

4. Install the packages using the native package tools for your system. For example, to install RPMs on Red Hat Enterprise Linux:

   ```
   ls *.rpm | egrep -iv -e devel -e debuginfo | xargs rpm -ivh
   ```

   Solaris tools can be used to install its packages.
5. Run **setup-ds-admin.pl** to configure a new instance.

   ```
   setup-ds-admin.pl
   ```

   See the *Directory Server Installation Guide* for more information about **setup-ds-admin.pl** script options and the Directory Server configuration interface.
6. The Password Sync packages available for download contain the **PassSync.msi** installer file. Download this file to the Windows machine, and then double-click the icon and go through the installer.

Installing through up2date or yum

Red Hat Enterprise Linux customers can simply install or update their packages using **up2date** or **yum**, using an account with entitlements for the Red Hat Directory Server 8.2 release.

1. Install the packages. For example, on Red Hat Enterprise Linux 5:

   ```
   yum install redhat-ds
   ```

2. Run **setup-ds-admin.pl** to configure a new instance.

   ```
   setup-ds-admin.pl
   ```

   See the *Directory Server Installation Guide* for more information about **setup-ds-admin.pl**

script options and the Directory Server configuration interface.

3. Password Sync packages must be downloaded from Red Hat Network.
    a. Log into Red Hat Network.
    b. Open the Red Hat Directory Server 8.2 channel in **Channels**, and go to the **Downloads** tab.
    c. Download the **PassSync.msi** and save it to a Windows machine.
    d. On the Windows machine, double-click the icon and go through the installer.

4.3. Upgrading to Directory Server 8.2

Red Hat Enterprise Linux systems support an in-place upgrade when moving from Red Hat Directory Server 8.1 to Red Hat Directory Server 8.2. To do this:

IMPORTANT

If there are any duplicate entries (based on duplicate DNs), then the upgrade process makes a copy of the database. It is possible, in an extreme case, that the upgraded database could be twice the size of the original database, until the duplicate antries are resolved. As a precaution, make sure there is enough disk space available for the upgrade, meaning that there is twice the current database size available.
If there is not enough disk space available, the upgrade process files with the error message *Failed to back up backend instance '<instance_name>'*.

1. Back up the current Directory Server. For example:

```
 cd /usr/lib/dirsrv/slapd-instance_name

 db2bak /var/lib/dirsrv/slapd-instance_name/bak/instance_name-
2009_04_30_16_27_56
```

2. Install or update the RPMs. For example:

```
yum update -y
```

This automatically updates the Red Hat Directory Server packages and all required packages.

Red Hat Directory Server 8.2 requires that all of the packages in the Red Hat Directory Server channel be updated. Running simply **yum update** updates all Red Hat Directory Server and Red Hat Enterprise Linux packages. To exclude packages from updating on your system, you can use **--exclude** *packages*, restrict the update to only the Red Hat Directory Server channel, or explicitly list the packages to update. Run **man yum** for a list of options.

3. Re-run the setup script with the **-u** option.

```
setup-ds-admin.pl -u
```

This updates the settings automatically, without having to migrate or re-configure the server.

4. Restart the Directory Server.

```
service dirsrv restart
```

NOTE

Manually restarting the server should only be required for Red Hat Enterprise Linux 4 systems. Other systems should restart automatically.

5. Verify that the packages have been properly updated by checking the version number on one of the Directory Server packages. For example:

```
rpm -qf /usr/sbin/setup-ds-admin.pl
redhat-ds-admin-8.2.0-0.el5dsrv
```

   Also restart the Directory Server Console to make sure that the version and build numbers are appropriately updated.

6. As part of migration, the DNs are encoded and updated to comply with RFC 4514. Verify that the databases were correctly updated by searching for an entry which could contain escaped characters; the DNs should be updated. For example, for a DN which was previously **cn="a=abc,x=xyz"**:

```
/usr/lib64/mozldap/ldapsearch -b "dc=example,dc=com" '(cn=\"*\")' entrydn
dn: cn=a\3Dabc\2Cx\3Dxyz,dc=example,dc=com
entrydn: cn=a\3dabc\2cx\3dxyz,dc=example,dc=com
```

   If the search results are correctly escaped, the database backups can be removed.

7. Any entries with duplicate DNs are processed and the duplicates are renamed with their unique ID in the new RDN. Check the error log for any warnings of duplicate entries (which will have the term *Duplicated entrydn* or *Duplicated entry* in the error messages), and then manually delete any duplicate entries.

   The procedure for this is described in Section 2.2, “No Longer Allowing Duplicate DNs”.

4.4. Migrating to Directory Server 8.2

Upgrading from Red Hat Directory Server 7.1 to Directory Server 8.2 requires migration. The migration process has a special script, **migrate-ds-admin.pl**, which copies the data and configuration from the 7.1 instance to the new 8.2 instance. For example, to migrate all 7.1 instances to 8.2 on the same machine:

```
migrate-ds-admin.pl --oldsroot /opt/redhat-ds
General.ConfigDirectoryAdminPwd=password
```

Additional migration scenarios are covered in the *Red Hat Directory Server Installation Guide*.

NOTE

Because of a known issue, Bugzilla #573889, remove any deprecated schema files from th Red Hat Directory Server 7.1 **schema** directory before running the migration script.

Migrated instances may encounter entries which had duplicate entry DNs with slightly different DN formats, related to Section 2.2, “No Longer Allowing Duplicate DNs”. After running the migration script, check the error logs for any warning messages that indicate duplicate entries:

```
[...] - import userRoot: WARNING: Skipping duplicate entry
"cn=uid\3Dtuser1\2Cou\3DOU0\2Co\3DO0,ou=People,dc=example,dc=com" found at line
35 of file "/opt/redhat-ds/slapd-ID/db/example.ldif"
```

Examine any duplicate entry messages to see if the resulting entry is acceptable. The import utility used during migration picks up the first entry and skips any subsequent duplicated entries. If necessary, edit the original LDIF file, and delete the unwanted entries. Run **`remove-ds-admin.pl`** to remove the newly-migrated server, and run the migration script again.

5. Basic Information about Red Hat Directory Server

This is some basic information for using and managing Directory Server. The Directory Server information is explained in much more detail in the *Administrator's Guide*.

Starting and Stopping the Directory Server and Admin Server

The Directory Server and Admin Server instances are started and stopped using basic service command line tools. For example, on Red Hat Enterprise Linux:

```
service dirsrv-admin start
service dirsrv start
```

Running just **`service dirsrv start`** starts all instances of the Directory Server on the host machine. To start a single instance, use the name of the instance in the command:

```
service dirsrv start example
```

Starting the Directory Server Console

To start the Directory Server Console, run the **`redhat-idm-console`** command.

```
redhat-idm-console
```

It is also possible to specify the user to log into the Console as using the **`-u`** and to give the URL to the Admin Server using the **`-a`** option.

```
redhat-idm-console -u "cn=Directory Manager" -a http://ldap.example.com:9830
```

Default Port Numbers

These are the default port numbers for the Directory Server and Admin Server:

- The standard LDAP port is **`389`**.
- The secure (SSL) LDAPS port is **`636`**.
- The Admin Server port is **`9830`**.

Tool Locations

The Mozilla LDAP tools used to manage Directory Server, such as **`ldapsearch`** and **`ldapmodify`**, are in the following directories, depending on platform:

- /usr/lib/mozldap6 on 32-bit Red Hat Enterprise Linux systems

- /usr/lib64/mozldap on 64-bit Red Hat Enterprise Linux systems

Some OpenLDAP tools are located in /usr/bin on Red Hat Enterprise Linux systems already; it is possible to manage Directory Server with these tools (always using **-x** to disable SASL by default) but this is not recommended.

Directory Server File Locations

Red Hat Directory Server 8.2 conforms to the Filesystem Hierarchy Standards. For more information on FHS, see the FHS homepage, http://www.pathname.com/fhs/. The files and directories installed with Directory Server are listed in the tables below for each supported platform.

Table 1. Basic Directory Locations

File or Directory	Location
Log files	/var/log/dirsrv/slapd-*instance*
Configuration files	/etc/dirsrv/slapd-*instance* /var/lib/dirsrv/slapd-*instance*
Instance directory	/usr/lib/dirsrv/slapd-*instance* on 32-bit systems /usr/lib64/dirsrv/slapd-*instance* on 64-bit systems
Database files	/var/lib/dirsrv/slapd-*instance*/db
Certificate and key databases	/etc/dirsrv/slapd-*instance*
Schema files	/etc/dirsrv/slapd-*instance*/schema
Runtime files	/var/lock/dirsrv/slapd-*instance* /var/run/dirsrv/slapd-*instance*
Tools	/usr/bin/ /usr/sbin/

UTF-8 and Language Support

Directory Server supports all international charactersets by default because directory data is stored in UTF-8. UTF-8 characters are fully supported for all DNs and DN components. Web services can be customized to display charactersets other than UTF-8, though UTF-8 and Latin-1 are the default for Directory Server web applications.

Directory Server can also use specified matching rules and collation orders based on language preferences in search operations.

The locales and charactersets supported by Directory Server are listed in more detail in Appendix D, "Internationalization," in the *Administrator's Guide*.

6. Bugs Fixed in 8.2

Along with new features, Directory Server 8.2 contains many bug fixes for all functional areas, features, and components in the directory service and associated tools, as well as the documentation. The complete list of bugs fixed in Directory Server 8.2 are listed in the tracking bug for this release, Bugzilla

434914. Many of the most important bugs are listed in Table 2, “List of Bugs Fixed in 8.2”.

Table 2. List of Bugs Fixed in 8.2

Bug Number	Description
195302	The global password policy was always in effect, even if a local password policy had been set.
196918	Some core schema elements were not compliant with the formats stated in RFC 2256.
201275	If a client bound to the server using the EXTERNAL method and a client certificate, the server skipped checking for the ***nsAccountLock*** setting.
457456	Improperly entering a ***uidNumber*** for a **posixUser** could escalate that user to root-level access. Attribute syntax validation compares any submitted attribute value against allowed attribute values, which should prevent this kind of escalation.
487425	The server process crashed after the changelog was moved.
490997	Some default ACIs in **o=netscaperoot** referenced obsoleted elements, like **nsconfigRoot=***. These references have been removed.
495073	When performing an in-place upgrade from Directory Server 8.0 to 8.1, new plug-in and schema entries were not written into the server configuration and had to be added manually.
496863	The **Construct** button in the Directory Server Console created incorrect referral URLs.
507460	Access log reported **notes=U** for VLV-indexed searches if there are no records to be found.
509201	When running a Directory Server 8.1 hub with a Directory Server 7.1 master, numerous err=32 messages were recorded on the hub whenever replication initiated. This was because DNs were not normalized between servers.
509472	Running **db2index** with the **all** did not reindex all the database backends correctly.
513172	No error messages were returned if the returned page size was greater than the ***nsslapd-sizelimit*** setting.
513308	When using SASL to secure the connection in chaining databases, the server used an empty principal name.
516305	When a modify operation was run with non-existent attributes or missing attribute values, the operation appeared to complete successfully, even though the entry was unchanged.

518112	If two threads attempted to evaluate an IP-based ACI at the same time, the server crashed with a segfault.
520483	If a new server instance attempted to register with a remote Configuration Directory Server when DHCP or DNS wasn't properly configured, the error message itself broke, which ultimately broke the installation process.
521108	Attempting to create a new role in some circumstances created an endless loop that caused the operation to fail.
531929	bvals could be set to NULL, but the server segfaulted on NULL values for some bvals.
536703	Migration failed if a synced user had a ***seeAlso*** value set to an entry outside the synced subtree.
549554	A full resynchronization process with Active Directory aborts if an entry had a multi-valued attribute.
554573	For SASL/EXTERNAL connections, ACIs were checking against the bind DN given by the bind request rather than the DN contained in the certificate map.
555970	If a replication operation attempted to access a view cache that was in use by another client, the server crashed.
574098	The Directory Server Console had a text field when adding the ***usercertificate*** attribute to a user, when it should have had a **Set Value** button to browse to the certificate file.
577384	The **remove-ds.pl** script threw a sh: START PIDFILE.*=: not found error on Solaris 9.
590931	Import operations used hardcoded **pages_limit** values regardless of the ***nsslapd-import-cache-autosize*** setting.
593067	If a directory already existed with the name **slapd-***serverID***.removed**, then an upgrade process failed because the old instance couldn't be written to the ***.removed** location.
593392	Running the setup script with the **--keepcache** option created a file with permissions that allowed any regular user to access it.

7. Security Updates

Bugzilla 732928: httpd: multiple ranges DoS

A flaw was discovered in the Apache HTTP server that could allow a remote attacker to make the **httpd**

process use an excessive amount of CPU time and system memory by crafting HTTP requests with a specially-crafted Range header. Detailed information is available in Bugzilla CVE-2011-3192 and through the Apache project security advisory at http://httpd.apache.org/security/CVE-2011-3192.txt.

On Red Hat Enterprise Linux systems, this problem can be adjusted by installing Errata RHSA-2011:1245, which updates the Apache HTTP server packages without requiring any changes to the Directory Server or Admin Server configuration.

The Admin Server HTTP server is included with the Solaris Red Hat Directory Server packages. Because neither Admin Server nor Directory Server use ranges, the Range headers in requests can be ignored without affecting their performance. On Solaris systems:

1. Open the Admin Server HTTP configuration file:

```
vim /etc/dirsrv/admin-serv/httpd.conf
```

2. For every module directive, add this line:

```
LoadModule headers_module /opt/fortitude/modules/mod_headers.so
```

3. After the modules section, add this line to disable ranges for the Apache HTTP server:

```
RequestHeader unset Range
RequestHeader unset Request-Range
```

4. Save the file.
5. Restart the Admin Server.

```
/etc/init.d/disrv-admin restart
```

8. Errata Updates

The following errata have been issued for Red Hat Directory Server, fixing important security and performance issues. The complete list of errata issued for Red Hat Directory Server 8.2 is available through Red Hat Network:

- Red Hat Enterprise Linux 5
- Red Hat Enterprise Linux 4

Table 3. Bugs Fixed in Errata Updates for Directory Server 8.2

Release Date	Errata Release	Bug Number	Description
January 24, 2012	RHBA-2012:0064	758978	The previous version of Red Hat Directory Server used the NSPR implementation of reader/writer locks (rwlocks). However, this implementation does not allow the use of re-entrant locks and consequent to this, an attempt to perform multiple concurrent searches with large search filters and many DN syntax attributes may have led to the server deadlock. With this update, the server has been adapted to use POSIX rwlocks on Linux platforms. As a result, deadlocks no longer occur in this scenario.
		767273	Due to excessive DN normalization, multiple concurrent searches with large search filters with many DN syntax attributes could cause the server to use an inordinate amount of CPU. This update introduces a new configuration attribute, nsslapd-normalize-nested-dn, which allows users to turn the DN normalization off, resolving this issue.
December 19, 2011	RHBA-2011:1835	748575	Repeated modrdn operations caused performance problems in replicated environments and caused the ns-slapd process to repeatedly hit 100% CPU usage.
		750622	SASL bind operations could cause the server to leak memory.
August 10, 2011	RHBA-2011:1146	709468	When performing an LDAP search operation using the Simple Paged Results Control, if the connection was left idle for longer than specified in the search operation's timelimit, the directory server timed out and closed the connection, and the console returned time out errors. With this update, when the client reads all of the results to completion, the server resets the search operation's time out and the idle connection is not closed until the server's own idle timeout threshold is reached.
		697694	In some specific circumstances under a heavy replication update load with multiple masters, the master's error log would sometimes record "Bad parameter to an LDAP routine," followed by "stop_fatal_error" and "requires administrator action" messages. With this update, these errors no longer occur.
June 15, 2011	RHBA-2011:0866	606920	If the client specified the "sizelimit" or "timelimit" option with the search request, the specified limit was not honored by the Directory Manager. This problem has been fixed so that the limit is now

			honored.
		520151	When the proxy authentication was used, the proxy user was unable to change the "userPassword" attribute of another user, although the proxy user had sufficient rights to do so. This update has fixed the problem so that the proxy user is now able to change the attribute.
		707015	Previously, disabling the use of SSLv3 with the FIPS Mode on was not supported so that Red Hat Directory Server had no way to explicitly disallow the use of SSLv3 and only use TLSv1 after the FIPS mode was enabled. This update adds the necessary support for disabling SSLv3 with the FIPS Mode on and thus fixes the problem.
February 22, 2011	RHSA-2011:0293	CVE-2011-0019	A flaw was found in the way Red Hat Directory Server handled simple paged result searches. If an unauthenticated user were able to send multiple simple paged search requests to Directory Server, it could cause the server to crash.
		CVE-2011-0022	When multiple Red Hat Directory Server instances were configured on the system to run under different unprivileged users, the Directory Server setup scripts set insecure permissions on the /var/run/dirsrv/ directory, which stores process ID (pid) files. A local user could use this flaw to manipulate the pid files in that directory, possibly preventing Directory Server instances from starting correctly, or causing the Directory Server init script to kill an arbitrary process when shutting down Directory Server.
		CVE-2011-0532	Multiple scripts set the LD_LIBRARY_PATH environment variable to an insecure value containing an empty path. A local user able to trick a user running those scripts (usually the root user) to run them while working from an attacker-writable directory could use this flaw to escalate their privileges via a specially-crafted dynamic library.
January 3, 2011	RHBA-2011:0003	614511	The DN normalization routines could possibly dereference a NULL pointer.
		640027	A DN with multi-valued RDNs could be incorrectly normalized if it contained an escaped '+' character.
		641944	The DN normalization routines would normalize non-DN attributes used in the RDN as if they contained a DN value. This resulted in incorrectly normalized values.
November 10, 2010	RHBA-2010:0874	644608	During an upgrade, the ancestorid could be rebuilt with an incorrect order, causing search

			results to be incorrect.
September 9, 2010	RHBA-2010:0692	612264	The ACL processing in the Directory Server would attempt to check the password modify rights for an entry before actually pulling the entry from the database. This meant that some ***userPassword*** modify operations failed, even if the ACLs were set to allow the operation.

9. Known Issues

The following are some of the most important known issues in Directory Server 8.2. If applicable, supported workarounds are also described.

Table 4. Known Issues in Directory Server 8.2

Bug Number	Description	Workaround
151705	The Admin Server Console is hard-coded to set all TLS ciphers to enabled. Disabling the TLS ciphers through the Console is not saved, and the ciphers are re-enabled when the Admin Server is restarted.	*Never* edit the Admin Server ciphers through the Console. Instead, edit the **`console.conf`** file directly. This file is located in **`/etc/dirsrv/admin-serv/`** directory.
182509	The changelog used for replication stores passwords in clear text in order to replicate them. In some contexts, this could be a security risk.	Enable fractional replication and specifically exclude the ***userPassword*** attribute from being replicated, which prevents passwords from being written to the changelog. For example: *nsds5replicatedAttributeList: (objectclass=*) $ EXCLUDE userPassword*
190862	Global syntax checking attributes should be enforced if the settings aren't configured in the local password policy. However, if both global and local password policies are configured, the global policies aren't being enforced as the default.	1. Enable global syntax checking. 2. Enable fine-grained password checking. 3. Edit the local password policy to contain all password syntax attributes. Set the values to something other than the default settings, as listed in the *Configuration, Command, and File Reference*. 4. Re-edit the local password policy with the desired values, even if they are the defaults.
470084	When updating from Berkeley DB libdb-4.4 to libdb-4.7, there can be problems migrating the data in the older database. This is indicated in the error logs with messages like: *libdb: Program version 4.7 doesn't match environment version 4.4*	Migrate to the newer Berkeley DB with this procedure: 1. Shut down the older database. 2. Still using the old version of Berkeley DB, run recovery on the database environment using the DB_ENV->open method or the db_recover utility. 3. With the DB_ENV->open method to run recovery,

		make sure that the Berkeley DB environment is removed using the DB_ENV->remove method or an appropriate system utility. 4. Archive the database environment for catastrophic recovery. 5. Recompile and install the new version of the application. 6. Force a checkpoint using the DB_ENV->txn_checkpoint method or the db_checkpoint utility. With the db_checkpoint utility, make sure to use the new version of the utility; that is, the version that came with the release of Berkeley DB to which you are upgrading. 7. Restart the application. **NOTE** When the Directory Server restarts, if it sees that the Berkeley DB version is newer than the one used for its database files, the server automatically starts the database with DBLAYER_CLEAN_RECOVER_MODE, which is similar to running the Berkeley DB db_recover utility.
472131 564448	Directory Server stores entry IDs in an ID list in a duplicate btree. If the ID list is very long, the internal database uses internal pages to sort the entries. When verifying database data, Berkeley DB's verify function returns *out-of-order key* errors because the	

	database verification does not differentiate between the duplicate btree ID list and the main tree entry pages. The database, then, incorrectly tries to compare the main database page to itself rather than the duplicate ID btree. This affects Directory Server client tools such as **`verify-db.pl`** and **`dbverify`**. This issue has been fixed in BerkeleyDB 4.8.26. However, the fix will not be available for Red Hat Enterprise Linux 4.	
517905	When Windows synchronization is enabled, if a user is moved from one subtree on Active Directory to another subtree, the user entry is not moved to the corresponding location on the Directory Server during the next synchronization.	
573889	Deprecated schema files, such as **`10presence.ldif`** are not removed automatically by the migration script (**`migrate-ds-admin.pl`**) when a Red Hat Directory Server 7.1 instance is migrated to Red Hat Directory Server 8.2. This causes migration to fail with this error: *Could not import the LDIF file '/tmp/nsrootJMtOFK.ldif' for the migrated database. Error: 256. Output: importing data ...* *[10/Mar/2010:13:12:44 -0700] dse - The entry cn=schema in file /etc/dirsrv/slapd-ldap/schema/60mozilla.ldif is invalid, error code 20 (Type or value exists) - attribute type nsAIMid: Does not match the OID "1.3.6.1.4.1.13769.2.4". Another attribute type is already using the name or OID* *[10/Mar/2010:13:12:44 -0700] dse - Please edit the file to correct the reported problems*	Remove the deprecated schema files from the *serverRoot***`/slapd-`***serverID***`/config/schema/`** directory first, then copy over the files and proceed with migration. To determine what files are deprecated, simply compare the contents of the old **`schema/`** directory to the new **`/etc/dirsrv/schema`**.

	and then restart the server.	

592022	DN formats in Directory Server 8.2 must comply with RFC 4514. This means that special characters (including quotation marks and commas) in a DN component must be escaped. To maintain backwards compatibility, migrated Directory Server entries will have encoded special characters in the DN. On Red Hat Enterprise Linux, DNs are updated automatically as part of installing the packages on Red Hat Enterprise Linux. However, on Solaris, the **setup-ds.pl** must be run to update DNs manually, and then the setup script is run to complete the updates for the server.	On Solaris only:
		1. Download the product binaries (from Red Hat Network or media) to the Directory Server installation directory.
		2. Unzip the package.
		`gunzip -dc filename.tar.gz | tar -xvof -`
		3. Stop the Directory Server and Admin Server.
		`/etc/init.d/dirsrv stop`
		`/etc/init.d/dirsrv -admin stop/`
		4. Remove the old packages.
		`pkgrm -n` ***DS_packages***
		5. Install the new packages.
		`pkgadd -d /path/to/`***DS_packages***`.sparcv9.pkg`
		6. Run **setup-ds.pl** with the **-u** option. This updates the DN formats in any migrated databases to be compliant with RFC 4514.
		`setup-ds.pl -u`
		7. Restart the Directory Server and Admin Server.
		`/etc/init.d/dirsrv start`
		`/etc/init.d/dirsrv -admin stop`
		8. Run **setup-ds-admin.pl** with the **-u**

		option to complete the upgrade process. `setup-ds-admin.pl -u`

596521	Import operations encounter fatal failures on some environments when trying to create an index for more than 200 attributes.	The failures occur because the ulimit setting on the machine is too small to accommodate the import operation. To avoid that error, set the ulimit value close to the system memory setting to allow the system to create more threads without causing the import to fail.
		First, check the current stack size:
		`ulimit -a`
		Then, change the ulimit value.
		`ulimit -s new_size`

608125	On Red Hat Enterprise Linux 4 64-bit systems, the SNMP MIB tables are not updated with all monitoring data, even if SNMP is properly configured and and the Directory Server SNMP service is running. The Directory Server MIB tables are properly updated on Red Hat Enterprise Linux 5 systems and on Red Hat Enterprise Linux 4 32-bit systems.	
612771	Older instances of Directory Server allowed entries with duplicate DNs with slightly different formats. During a migration or upgrade process, a warning about the duplicate entry is recorded in the error logs.	For 7.1 migrations, the migration process keeps the first entry and ignores any duplicates. To change this, the original LDIF file must be edited and then the migration script must be re-run. For in-place upgrades, both entries are written into the new database, and the duplicate entry is renamed with its nsuniqueid value in the DN. Administrtors can go in and select which entry to keep.

616598	The **`console.conf`** file for the Admin Server is overwritten during the upgrade process on Sun Solaris.	Save the original **`console.conf`** file and manually copy it in place.
		1. Download the product binaries (from Red Hat Network or media) to the Directory Server installation directory.
		2. Unzip the package.
		`gunzip -dc filename.tar.gz | tar -xvof -`
		3. Stop the Directory Server and Admin Server.
		`/etc/init.d/dirsrv stop`
		`/etc/init.d/dirsrv -admin stop/`
		4. Back up the old **`console.conf`** file.
		`cd /etc/dirsrv/admin-serv ; cp -fp@ console.conf console.conf.save`
		5. Remove the old packages.
		`pkgrm -n` ***`DS_packages`***
		6. Install the new packages.
		`pkgadd -d /path/to/`***`DS_packages`***`.sparcv9.pkg`
		7. Restore the **`console.conf`** file.

```
cd
/etc/dirsrv/admin-
serv ; cp -fp@
console.conf
console.conf.new
cp -
fp@console.conf.sa
ve
console.conf.new
```

8. Run **`setup-ds.pl`** with the **`-u`** option.

```
setup-ds.pl -u
```

9. Restart the Directory Server and Admin Server.

```
/etc/init.d/dirsrv
start
/etc/init.d/dirsrv
-admin stop
```

10. Run **`setup-ds-admin.pl`** with the **`-u`** option to complete the upgrade process.

```
setup-ds-admin.pl
-u
```

621727	The DNA Plug-in only works on a single backend; it cannot manage number assignments for multiple databases. The DNA plug-in uses the sort control when checking whether a value has already been manually allocated outside of the DNA Plug-in. This validation, using the sort control, only works on a single backend. Attempting to add a user or attribute in a distributed database with the DNA Plug-in configured fails with an operations error.	

	`add description: group add for DNA Plugin test adding new entry "cn=User,ou=People,dc=example,dc=com" ldap_add: Operations error (1) additional info: Allocation of a new value for gidnumber failed! Unable to proceed.`
	
	The error log contains a message that the sort control used with the DNA operations could not be processed.
	
	`[04/Aug/2010:11:18:59 -0400] - ERROR: The sort control cannot be processed when more than one backend is involved. VLV indexes that will never be used should be removed.`	

625950	When audit logging is enabled, changing the ***nsslapd-rootpw*** attribute for the Directory Manager password is logged to the audit log in cleartext. The audit log records the entire modify operation. For example: `dn: cn=config changetype: modify replace: nsslapd-rootpw nsslapd-rootpw: secret` User password changes are not logged in cleartext, but in hashed form.	Access to the audit log should be limited to the Directory Server user (**nobody**) and the system's root user. By default, the audit log permissions setting is **0600** and the log directory's setting is **0770**. Both the log directory and log file are owned by the Directory Server user (**nobody**).
713062	The Directory Server will successfully import entries with invalid entry USN values, which causes an unexpected ***lastusn*** value. The ***entryUSN*** attribute only accepts integer values. If an entry is imported with an ***entryUSN*** attribute with an	Check any LDIF file that is going to be imported into the directory and make sure that any ***entryUSN*** attributes have a valid, integer value before importing.

	invalid value, the entry is still imported successfully and the invalid attribute value is added to the entry USN index. Additionally, the ***lastusn*** value for the server is set to **0**. What should happen is that the import operation should fail and the ***lastusn*** value should be set to **-1**, indicating a failure.	